



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/409,617	10/01/1999	DAVID MICHAEL SHACKELFORD	TU9-99-029	5644

46917 7590 12/13/2005

KONRAD RAYNES & VICTOR, LLP.
ATTN: IBM37
315 SOUTH BEVERLY DRIVE, SUITE 210
BEVERLY HILLS, CA 90212

EXAMINER

LANIER, BENJAMIN E

ART UNIT PAPER NUMBER

2132

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/409,617	Applicant(s) SHACKELFORD, DAVID MICHAEL	
	Examiner Benjamin E Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 November 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-40 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-40 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 October 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
 If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
 * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
 a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendments filed 07 November 2005 amends claims 1, 4, 12, 16, 19, 25, 27,
30. Applicant's amendment has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments, filed 07 November 2005, with respect to the amended claim limitations have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further search and consideration required by the amendments to the claims, a new ground(s) of rejection is made in view of Davis, U.S. Patent No. 5,473,692.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 2, 8-14, 16, 17, 21-28, 34-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis, U.S. Patent No. 5,473,692. Referring to claims 1, 16, 27, Davis discloses a system for computer software license enforcement wherein a certification agent contains a storage device of authentic key pairs (Col. 7, lines 30-64), which meets the limitation of a first computer system, maintaining keys of computer systems authorized to access software to be distributed. The hardware/first agent of the requester transmits an authentication device certificate to the certification system/second agent in order to access software (Col. 8, lines 33-36), which meets the limitation of a second computer system, receiving a request for software

Art Unit: 2132

from a second computer system. The second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49), which meets the limitation of generating a message, encrypting the generated message, transmitting the encrypted message to the second computer system. The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of transmitting the encrypted message to the second computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response, decrypting the encrypted response with the determined key if there is one determined key. The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60), which meets the limitation of determining whether the decrypted response includes a part of the generated message transmitted to the second computer system. If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of the second computer system is authorized to access the software if the decrypted response includes the part of the generated message, permitting the second computer system access to the software after determination that the second computer system is authorized to access the software. If the response message does not match the original challenge then the communications are terminated and no valid license token is transmitted (Col.

8, lines 60-61), which meets the limitation of the second computer system is not authorized to access the software if the decrypted response does not include the part of the generated message transmitted to the second computer system.

Referring to claims 12, 25, Davis discloses a system for computer software license enforcement wherein a certification agent contains a storage device of authentic key pairs (Col. 7, lines 30-64). The key pairs are transmitted to the certification agent (Col. 7, lines 44-45), which meets the limitation of providing a key to the first computer system capable of decrypting an encrypted response from the second computer system. The hardware/first agent of the requester transmits an authentication device certificate to the certification system/second agent in order to access software (Col. 8, lines 33-36), which meets the limitation of transmitting a request for the software to the first computer system. The second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49), which meets the limitation of receiving an encrypted message from the first computer system. The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of processing the encrypted message to generate a response message including part of the encrypted message, encrypting the response message, transmitting the encrypted response message to the first computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of the encrypted response message is capable of being decrypted by the provided key at the first computer system. The second agent decrypts the

response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of receiving access to the requested software in response to the encrypted response message.

Referring to claims 2, 13, 17, 28, Davis discloses that the software being requested is a software application (Col. 9, lines 15-22), which meets the limitation of the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

Referring to claims 8, 9, 21, 22, 34, 35, Davis discloses that the second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message, wherein the encrypting the message comprises encrypting the message with a private key of the first computer system that is

Art Unit: 2132

the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the maintained keys comprise public keys from the authorized computer systems, wherein processing the encrypted response further comprises decrypting the encrypted response with one of the maintained public keys.

Referring to claims 10, 23, 36, Davis discloses that the challenge also includes a digital certificate (Col. 8, lines 33-35), which meets the limitation of configuration data.

Referring to claims 11, 24, 37, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49), which meets the limitation the generated message is encrypted with a private key of the first computer system, wherein the first computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system. The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54). The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of the encrypted response is encrypted with a private key of the second computer system, wherein the maintained keys comprise public keys from authorized computer systems.

Referring to claims 14, 26, 39, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49). The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key, encrypting the decrypted message with the second computer system's private key, transmitting the message encrypted with the second computer system's private key to the first computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of wherein the key made available by the second computer system that is capable of decrypting the received encrypted response comprises the public key associated with the second computer system.

Referring to claim 38, Davis discloses a system for computer software license enforcement wherein a certification agent contains a storage device of authentic key pairs (Col. 7, lines 30-64). The hardware/first agent of the requester transmits an authentication device certificate to the certification system/second agent in order to access software (Col. 8, lines 33-36), which meets the limitation of transmitting a request for the software to the first computer system. The second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49), which meets the limitation of receiving an encrypted message from the first computer system. The first agent

Art Unit: 2132

receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of processing the encrypted message to generate a response message, transmitting the response message to the first computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of receiving access to the requested software in response to the response message.

Referring to claim 40, Davis discloses that the challenge also includes a digital certificate (Col. 8, lines 33-35), which meets the limitation of configuration data.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

Art Unit: 2132

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 3, 18, 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692. Referring to claims 3, 18, 29, Davis discloses that if the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22). Davis does not specify how the software is distributed. Davis does suggest that electronic distribution systems for software are a viable distribution option (Col. 2, lines 26-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to electronically distribute the actual software application at the time of authentication in the system of Davis in order to increase convenience and reduce distribution costs as taught by Davis (Col. 2, lines 27-29).

8. Claims 4, 15, 19, 30 and rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692, in view of Schneier. Referring to claims 4, 15, 19, 30, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49). The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54). The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The

second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of determining whether the response includes the component included with the message. Davis does not disclose that the challenge is random. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the challenge in Davis to a random challenge in order for the challenge to be unpredictable as taught by Schneier (Page 45). According to Schneier (Page 45), it is computationally infeasible to predict what the next random bit will be, given complete knowledge of the algorithm or hardware generating the sequence and all of the previous bits in the stream. This is beneficial to Davis because the issuer of the challenge would want the challenge to be unpredictable so that the resultant authentication was genuine.

9. Claims 5, 6, 31, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692, in view of Komura, U.S. Patent No. 5,994,307. Referring to claims 5, 6, 31, 32, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49). Davis does not disclose that the challenge contains a time stamp. Komura discloses a packet transmission system wherein time stamp offset values are attached to data packets (message)(Col. 7, lines 22-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use time stamp offset values in the software licensing system of Davis, for synchronizing purposes taught in Komura (Col. 6, lines 40-67).

Art Unit: 2132

10. Claims 7, 20, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692, in view of Takahashi, U.S. Patent No. 6,195,432. Referring to claims 7, 20, 33, Davis discloses that if the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22). Davis does not specify how the software is distributed. Davis does suggest that electronic distribution systems for software are a viable distribution option (Col. 2, lines 26-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to electronically distribute the actual software application at the time of authentication in the system of Davis in order to increase convenience and reduce distribution costs as taught by Davis (Col. 2, lines 27-29). Davis does not disclose or suggest that the software is automatically installed after electronic distribution. It would have been obvious to one of ordinary skill in the art to automatically install the transmitted software in Davis in order to assist users who are not accustomed to handle a personal computer as taught in Takahashi (Col. 3, lines 57-64).

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period

Art Unit: 2132

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

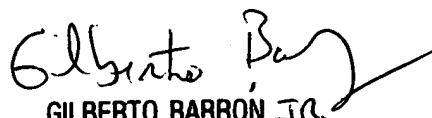
12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100